CLAIMS

1. Method for authenticating a portable object (7) comprising information processing means (8) and information storage means (9, 10), the information storage means containing at least one code (i) defining operations capable of being executed by the portable object, as well as a one-way function, characterized in that it comprises the step that consists of sending the portable object an order (31, 32i-34i, 35, 36) so that the latter executes a calculation of a result by applying to said one-way function at least part of said code (i), this result being used to decide whether or not the portable object is authentic.

2. Method according to claim 1, wherein said result enters into the implementation of a given operation, this operation being performed successfully only when the portable object (7) is authentic.

3. Method according to claim 2, wherein said given operation comprises a decryption operation, said result making it possible to produce an associated decryption key.

4. Method according to claim 1, wherein said code part (i) used in the calculation comprises a machine code part.

5. Method according to claim 1, wherein the portable object (7) contains a so-called "real" code defining operations designed to be executed by the portable object, and a so-called "dummy" code defining operations not designed to be executed by the portable object, said code part used in the calculation comprising a dummy code part.

6. Method according to claim 1, wherein said order (31, 32i-34i, 35, 36) is sent to the portable object repeatedly during its life, prior to the execution by the latter of said operations.

7. Method according to claim 1, wherein said code part (i) used in the calculation is defined by a start address (32i) and an end address (33i) in the information storage means, said addresses being sent to the portable object.

8. Method according to claim 1, wherein said code (i) comprises a set of binary words, said code part used in the calculation being defined by a subset of binary words comprising the binary words distributed in the information storage means at a determined pitch (34i), said pitch being sent to the portable object.

9. Method for having a portable object (7) execute a sensitive operation, the portable object comprising information processing means (8) and information storage means (9, 10), the information storage means containing at least one code (i) defining operations capable of being executed by the portable object, as well as a one-way function, characterized in that it comprises the step that consists of sending the portable object an order (31, 32i-34i, 35, 36) so that the latter executes a calculation of a result by applying to said one-way function at least part of said code (i), said result entering into the implementation of said sensitive operation, this operation being performed successfully only when the portable object (7) is authentic.

10. Method according to claim 9, wherein said code part (i) used in the calculation comprises a machine code part.

11. Method according to claim 9, wherein the portable object contains a so-called "reel" code defining operations designed to be executed by the portable object, and a so-called "dummy" code defining operations not designed to be executed by the portable object, said code part used in the calculation comprising a dummy code part.

12. Portable object comprising information processing means (8) and information storage means (9, 10), the information storage means containing at least one code (i) defining operations capable of being executed by the portable object, as well as a one-way function, characterized in that it comprises means for executing a calculation of a result by applying to said one-way function at least part of said code.

13. Portable object according to claim 12, wherein said code part (i) used in the calculation comprises a machine code part.

14. Device (1) comprising information processing means (2) and information storage means (3, 4) and designed to communicate with a portable object (7) in order to authenticate the latter, the portable object comprising information processing means (8) and information storage means (9, 10), the information storage means of the portable object containing at least one code (i) defining operations capable of being executed by the portable object, as well as a one-way function, characterized in that it comprises means for sending the portable object an order (31, 32i-34i, 35, 36) so that the latter executes a calculation of a result by applying to said one-way function at least part of said code (i) of the portable object.

15. Device according to claim 14, wherein said code part (i) used in the calculation comprises a machine code part.